Information Security Leads

Victorian Protective Data Security Framework and Standards

Overview

This information sheet provides guidance on the role of information security leads and implementing the Victorian Protective Data Security Framework and Standards.

Part 4 of the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**) applies to thousands of Victorian Public Sector (**VPS**) organisations that deliver different services or functions on behalf of the government.

Each organisation will employ a range of management structures to govern and protect public sector information, and support the delivery of efficient, effective and economic information security practices.

While accountability for adhering to the Victorian Protective Data Security Standards (the **Standards**) rests with the public sector body Head, they need to be supported by personnel who are appropriately skilled, resourced and empowered.

Managing an information security work program and organisational reporting

Given the diverse nature of the VPS, OVIC does not prescribe a specific role or group that should be tasked with managing information security, or organisational reporting obligations. Instead, OVIC recommends organisations adopt a collective effort to manage the internal security program, drawing insights and representation from all areas of the business.

Establishing a cross-functional information security committee or workgroup

OVIC recommends establishing a cross-functional work group, with representatives from across the business who can bring insights from their respective areas and help with communicating to a range of stakeholders[1].

Representatives may include personnel from:

- Executive, corporate, legal or procurement groups responsible for addressing security governance requirements, third-party arrangements and contractual arrangements;
- Risk managers who assist with integrating information security risks into the organisation's overall risk management framework;
- Chief Information Officers (CIOs), information or records managers who assist with identifying information holdings across the organisation;
- HR representatives who provide advice and input into personnel security matters;
- IT teams that support the delivery of ICT security initiatives;
- Internal auditors responsible for managing assurance programs on behalf of the organisation; and

[1] For smaller organisations, a cross-functional committee or workgroup may not be appropriate, given the limited number of personnel available to participate. In these instances, the information security lead should coordinate these activities.

- Facilities managers who provide advice and input into the physical security needs of the business.

Involving representatives from across the organisation can help develop and subsequently deliver information security programs that reflect the varying operational needs of the organisation.

Organisations should take a holistic approach in scoping their information security program, to properly manage their information security risks.

Nominating an information security lead

Element E1.050[2] of the Standards requires each public sector body Head to nominate an *information security lead* (**lead**) for their organisation. E1.050 also requires an organisation to notify OVIC of any changes to the lead, providing an alternative point of contact if they move roles or cease working for the organisation.

Role of an information security lead

An information security lead acts as a central point of contact for OVIC, helping deliver important information security messages and updates relating to the Framework and Standards. They can also help coordinate or guide the implementation of the Standards on behalf of the organisation.

In addition, information security leads may receive invites from OVIC for targeted training and awareness sessions, access to Special Interest Groups (**SIGs**) and other outreach initiatives led by the OVIC Information Security team.

Management structures and responsibilities

To find out more about potential management structures and security roles and responsibilities of organisations, refer to the advice outlined *Policy 2 of the Commonwealth Protective Security Policy Framework (PSPF) – Management structures and responsibilities*[3].

Further Information

Contact Us

t: 1300 00 6842
e: security@ovic.vic.gov.au
w: ovic.vic.gov.au

Disclaimer

[2] Standard 1 (Information Security Management Framework), Element E1.050

[3] Refer to https://www.protectivesecurity.gov.au/governance/management-structures-and-responsibilities/Pages/default.aspx for more information